Conjugation

(Example of a group action)

$$\varphi : G \times G \longrightarrow G$$

$$\varphi(g,h) \longmapsto ghg^{-1}$$

1) $\varphi(e,h) = ehe^{-1} = h$

2) $\varphi(g_1, \varphi(g_2,h)) = g_1(g_2hg_2^{-1})g_1^{-1}$

$$= g_1g_2\, h\, (g_1g_2)^{-1}$$

$$= \varphi(g_1g_2, h)$$

$$\text{Stab}_h = \{g \in G \mid ghg^{-1} = h\}$$

$$= \{g \in G \mid gh = hg\}$$

(also known as centralizer)

$$\text{Orbit}(h) = \{ghg^{-1} \mid g \in G\}$$

(also known as conjugacy class)

Observation: Conjugacy classes are disjoint.

If $h_1 \neq g h_2 g^{-1}$ for any $g \in G$, then we want to show that $\text{Orbit}(h_1) \cap \text{Orbit}(h_2) = \phi$

Say $x \in \text{Orbit}(h_1)$
$x \in \text{Orbit}(h_2)$

$$x = g_1 h_1 g_1^{-1} = g_2 h_2 g_2^{-1}$$

$$\Rightarrow g_2^{-1} g_1 h_1 g_1^{-1} g_2 = h_2$$

$$\Rightarrow g_2^{-1} g_1 h_1 (g_2^{-1} g_1)^{-1} = h_2$$

$$\Rightarrow h_2 \in \text{Orbit}(h_1)$$

Contradiction!

$$G = \bigsqcup \text{Conjugacy classes}$$

$$= C_1 \sqcup C_2 \sqcup \cdots \sqcup C_R$$

$$|G| = |C_1| + |C_2| + \cdots + |C_R|$$

↳ Class equation of G.

Qn: If G is abelian, what is its class equation?

Qn: How many 1's appear in a class equation?

Centre of a group

$$Z(G) = \{ x \in G \mid gxg^{-1} = x \text{ for all } g \in G \}$$

$$|G| = \underbrace{1 + 1 + \cdots + 1}_{|Z(G)| \text{ times}} + - - -$$

Permutation Groups

$$|S_2| = 1 + 1$$

$$S_3 = \{e\}, \{(123), (132)\}, \{(12), (23), (13)\}$$

$$|S_3| = 1 + 2 + 3$$

Lemma: $\sigma, \tau \in S_n$ are in same conjugacy class $\iff$ they have same cycle type.

Pf: Example: $(12345)(67)$

$$\sigma (12345)(67)\sigma^{-1}$$

$$\underbrace{\sigma(12345)\sigma^{-1}}_{\substack{\text{cycle of} \\ \text{length} \\ 5}} \; \underbrace{\sigma(67)\sigma^{-1}}_{\substack{\text{cycle of} \\ \text{length} \\ 2}}$$

So, $\sigma\tau\sigma^{-1}$ has same cycle type for $\sigma, \tau \in S_n$.

$\Leftarrow$: Suppose σ_1, σ_2 have same cycle type.

Let's construct an element $\tau \in S_n$ such that $\tau\sigma_1\tau^{-1} = \sigma_2$

$\sigma_1 = (1\,2\,3\,4\,5)$

$\sigma_2 = (1\,4\,5\,3\,2)$

$\tau(1) = 1 \quad \tau(2) = 4 \quad \tau(3) = 5$

$\tau(4) = 3 \quad \tau(5) = 2$

$\tau = (2\,4\,3\,5)$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$\sigma_1\tau(4)$

$\tau(4)$

$\tau\sigma_1(4)$

$$\sigma_2 = \begin{pmatrix} 1 & 4 & 5 & 3 & 2 \end{pmatrix}$$

$\sigma_2\tau(4)$

$$\sigma_2 \circ \tau(i) = \tau\sigma_1(i) \quad \forall\, i \in \{1, 2, \dots, n\}$$

True in general, as well.

Exc: let's work out a class equation for S_4.

An application : p- groups

Defn: A finite group G is called p-group $\iff |G| = p^e$, $e > 0$.

Lemma: The center of a p-group is not trivial, i.e $|Z(G)| > 1$.

Proof: Class equation of G is

$$|G| = |C_1| + |C_2| + \cdots + |C_k|$$

Suppose $|Z(G)| = 1$

$$\Rightarrow \quad |G| = 1 + |C_2| + \cdots + |C_k|$$

For each C_i, $i \in \{2, 3, \ldots, k\}$

$$|C_i| \mid |G| \quad \text{and} \quad |C_i| > 1$$

So, $p \mid |C_i|$

$$|G| = 1 + \text{multiple of } p$$

This is contradiction.

Lemma: Let G be a group of order p^2. Then G is abelian.

Pf: We know that $|Z(G)|$ is p or p^2.
We want to show that $|Z(G)| = p^2$.
Suppose not.
Choose any $x \in G$ such that $x \notin Z(G)$.

$$Z(G) \subseteq \text{Centralizer}(x) \subseteq G$$
$$\text{Centralizer}(x) = \{g \in G \mid gx = xg\}$$

Order of Centralizer is either p or p^2

p: Contradiction

p^2: $G = \text{Centralizer}(x)$
$\Downarrow$
G is abelian.

Corollary: If G is a group of order p^2, then G is either isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Pf: (Case I:) If G has at least one element of order p^2, then G is cyclic $\Rightarrow$ G is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$

(Case II:) No element has order p^2.

Choose $x \in G$, such that order of $x = p$.

Let H be subgroup of G generated by x.

Choose $y \notin H$ of order p.

Let K be subgroup of G generated by y.

$$H \cap K = \{1\}$$

$$\Rightarrow HK \cong H \times K$$

$$\Rightarrow HK = G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

An application of group action : Sylow Theorems

(FIRST SYLOW THM:)

Let G be a finite group.
Let p be a prime that divides $|G|$.
Say $|G| = p^e n$, $p \nmid n$.
Then G has at least one subgroup of order p^e.

Proof: Consider $S = \left\{ \begin{array}{l} \text{Subsets of } G \text{ that} \\ \text{have exactly } p^e \\ \text{elements} \end{array} \right\}$

$$|S| = \binom{p^e n}{p^e} \equiv n \pmod p$$

Let us compute $|S|$ using group actions.

$$G \times S \longrightarrow S$$
$$(g, A) \longmapsto gA$$

This is a group action.

Suppose S has r orbits with respect to this action, say $S_1, S_2, \ldots, S_r$.

then $S = S_1 \sqcup S_2 \sqcup \cdots \sqcup S_r$

$\Rightarrow |S| = |S_1| + |S_2| + \cdots + |S_r|$

If $p \mid |S_i| \ \forall i \Rightarrow p \mid |S|$

but this is not possible.

So, there is at least one S_i such that $p \nmid |S_i|$. Choose one such S_i.

For $t \in S_i$, $\dfrac{|G|}{|Stab_t|} = |S_i|$

$$|G| = |S_i| \, |Stab_t|$$

Since p does not divide $|S_i| \Rightarrow |Stab_t| = p^e$

and Stabilizer is a subgroup

So, there exists at least one subgroup of order p^e.

Corollary: Let G be a finite group. Let p be a prime such that $p \mid |G|$. Then G contains an element of order p.

Pf: Say $|G| = p^e m \quad p \nmid m$.

There exists a subgroup H s.t

$$|H| = p^e.$$

Choose any $x \in H$, $x \neq e$.

Say $\text{order}(x) = p^k \quad k \leq e$.

$$\text{order}\left(x^{p^{k-1}}\right) = p.$$

Exc: What are all groups of order 6?